ABSTRACT OF THE DISCLOSURE

A cryptographic method using dual encryption keys and a wireless local area network (LAN) system therefor includes (a) generating a first group key in N wireless terminals forming an ad-hoc group, where N is equal to or greater than two, (b) generating a second group key in a main wireless terminal to perform a key distribution center function among the N wireless terminals, and transmitting the second group key to (N-1) sub wireless terminal, and (c) encoding data using the second group key, and transmitting the encoded data between the N wireless terminals. Data security in a wireless LAN system of an ad-hoc network is increased by creating a first group key having a low frequency of use using a group password, and using a random key generation algorithm to create, distribute, and modify a second group key in a wireless terminal functioning as a key distribution center.